(FILE 'USPAT' ENTERED AT 15:16:27 ON 15 MAR 1997)

~~L1 0 S 395/CALS~~

L2 35847 S 395/CLAS

~~L3 0 S L2 AND REALTIONAL DATABASE#~~

L4 501 S L2 AND RELATIONAL DATABASE#

L5 3 S L4 (P)TRAITS

=> s l4 and fingerprint

2112 FINGERPRINT

L6 1 L4 AND FINGERPRINT

=> s l4 and authentication
          1461 AUTHENTICATION
L8   5 L4 AND AUTHENTICATION
=> d 1- ab

US PAT NO: 5,542,024 [IMAGE AVAILABLE] L8: 1 of 5

ABSTRACT:
The specification describes a Graphically Used Expert System Tool, which is a computer program which enables a non-computer literate expert (the developer) to develop an expert system for non-expert users. A plurality of standardized data records and screen displays are linked together by the developer using simplified entry blanks and standardized icons which implement program functions. The developer enters segments of knowledge, which may be statements or questions on each data record, and links it to one to six other data records to form a disjoin logic set. The plurality of knowledge segments and the way in which they are linked together as exit option actions form a cognitive map which represents the natural thought process of the expert developer, thus eliminating the need for traditional deep thought analysis or "if then" inference rules and logic. By providing DOS commands, ARC commands, ARC variables or List processing at each exit option, the developer is provided with a tool which will invoke one or more of a plurality of functional program objects in response to a single user selection.

US PAT NO: 5,513,126 [IMAGE AVAILABLE] L8: 2 of 5

ABSTRACT:
A method for a sender to automatically distribute information to a receiver on a network using devices (such as printers and facsimile machines) and communication channels (such as electronic mail) defined in a receiver profile. The receiver profile establishes the properties and mode for receipt of information for receivers on the network and the profile is published in a network repository for all network users or is accessible by selected groups or individuals on the network. Receivers have additional control over network senders by defining an information filter which further controls sender channel access (to a receiver) by defining some channels as having priority of access such as direct or delayed access, as well as selectively permitting senders to override the receiver profile. Consequently, receiver profiles provide a variable receiver definable link to senders using multiple forms of media as well as multiple hardware platforms and network configurations.

US PAT NO: 5,355,474 [IMAGE AVAILABLE] L8: 3 of 5

ABSTRACT:
Apparatus for an integrated architecture for an extended multilevel

secure database management system. The multilevel secure database management system processes security constraints to control certain unauthorized inferences through logical deduction upon queries by users and is implemented when the database is queried through the database management system, when the database is updated through the database management system, and when the database is designed using a database design tool.

US PAT NO: 5,261,102 [IMAGE AVAILABLE] L8: 4 of 5

ABSTRACT:
A method and computer system are disclosed for determining the access privileges currently held by a database user with respect to objects in the database. The steps of the method are: (a) requesting a determination of those objects to which a given user has access privileges; (b) automatically determining those objects to which the user has direct access privileges; and (c) automatically determining those objects to which the user has indirect access privileges. This last step (c) is accomplished by (1) automatically determining all access groups to which the user belongs; and (2) automatically determining those objects to which those access groups, determined in step (1), have access privileges.

US PAT NO: 5,113,499 [IMAGE AVAILABLE] L8: 5 of 5

ABSTRACT:
A security access management system for a packet switched data communications network has access management apparatus operatively associated with the packet switches at each entry point of the network. The access management apparatus includes an administrative host processor for examining user terminal authorization information in packets received at the associated packet switch for transmission through the network to destination addresses for the packets. A database associated with the administrative host stores information including levels of authorization of the user terminals for the respective entry point of the network for access to specified destinations, as pre-assigned by the network customer. Also included in the access management apparatus is a validation host processor which responds to comparisons between the user terminal authorization information contained in the packet and the pre-assigned level of authorization for the same user terminal, and, if they correspond, to grant access by that user terminal through the associated packet switch to the destination address with which a communication session is requested; or, if they differ, to deny such access. The access management apparatus is located remote from the user terminals using the particular entry point for the network.
=

L8 Relational Database + Authentication

=> d kwic

US PAT NO: 5,542,024 [IMAGE AVAILABLE] L8: 1 of 5
US-CL-CURRENT: **395/356**, **76**, **352**

SUMMARY:

BSUM(24)

(e) . . . the GUI in response thereto. This feature of the invention allows the non-computer literate expert to create a relatively complex **relational** **database** structure with forward and backwards chaining with no knowledge of the script commands or code needed to create the data. . .

DETDESC:

DETD(6)

The database manager 12 is preferably a **relational** **database**, but may also be a B-tree database, a network database, a hierarchal database, a series of seeks, or a flat file database. A **relational** **database** will provide the smallest and most compact data structure.

DETDESC:

DETD(88)

The . . . use of common encryption algorithms such as the DES, data encryption standard, or other algorithms as discussed in Privacy and **Authentication**: An Introduction to Cryptography by Diffie and Hellman, IEEE, Vol. 67, No. 3 March, 1979.

CLAIMS:

CLMS(28)

28. An information processing system as claimed in claim 1 wherein said first means is selected from the group of: a **relational** **database**, a B-tree database, a network database, a hierarchal database, a series of seeks, or a flat file database.
=> d kwic 2-

US PAT NO: 5,513,126 [IMAGE AVAILABLE] L8: 2 of 5
US-CL-CURRENT: 364/514A; 358/402, 407; **395/200.02**

SUMMARY:

BSUM(4)

Protocols . . . Xerox System Integration Standard, Xerox Corp., Stamford, Conn., December 1981, XSIS-038112; Clearinghouse Protocol, Xerox Corp., Stamford, Conn., April 1984, XSIS-078404; **Authentication** Protocol, Xerox Corp., Stamford, Conn., April 1984, XSIS-098404; Filing Protocol, Xerox Corp., Stamford, Conn., May 1986, XNSS-108605. Another example of. . .

DETDESC:

DETD(6)

Referring . . . station 4 with public, shared and/or private data storage that is differentiated by user access rights. The server 14 includes **relational** **database** system 17, network administration system 18, mail system 19 (e.g. email, voice mail) and data storage and retrieval system 20, and can be physically configured using optical drives, hard drives, floppy drives and/or tape drives. The **relational** **database** system 17 provides systems with fast query and retrieval of data.

US PAT NO: 5,355,474 [IMAGE AVAILABLE] L8: 3 of 5
US-CL-CURRENT: **395/609**; 364/274, 282.1, 283.3, 283.4, 286.4, 286.5, 286.6, DIG.1; 380/4, 25

SUMMARY:

BSUM(7)

In contrast, the work reported in Thuraisingham, B., December 1987, "Security Checking in **Relational** **Database** Management Systems Augmented with Inference Engines," Computers and Security, Volume 6, No. 6.; Thuraisingham, B., August 1990, The Use of. . .

SUMMARY:

BSUM(23)

The . . . processor, update processor and database design tool are separate modules, they all constitute the solution to constraint processing in multilevel **relational** **databases**; these three approaches provide an integrated solution to security constraint processing in a multilevel environment. In the architecture shown in. .

SUMMARY:

BSUM(26)

The . . . a query processor is shown in FIG. 2. This architecture can be regarded as a loose coupling between a multilevel **relational** **database** management system and a deductive manager. The deductive manager is referred to as the query processor. It operates on-line.

SUMMARY:

BSUM(27)

An . . . the update processor is shown in FIG. 3. This architecture can be regarded as a loose coupling between a multilevel **relational** **database** management system and a deductive manager. The deductive manager is referred to as the update processor. It can be used. . .

DETDESC:

DETD(52)

The . . . a limited set of inference strategies. Nevertheless it is a useful prototype which enhances the security of existing multilevel secure **relational** **database** management systems. In this section, we discuss the techniques that we have used to implement the security policy. They are:. . .

DETDESC:

DETD(54)

Query . . . been used in the past to handle discretionary security and views. Stonebraker, M., and E. Wong, 1974j, "Access Control in **Relational** **Database** Management Systems by Query Modification," Proceedings ACM National Conference, New York, N.Y. This technique has been extended to include mandatory. . .

DETDESC:

DETD(88)

(ii) The second alternative is to augment a **relational** **database** management system with a theorem prover implemented in Prolog. The advantages of augmenting a **relational** **database** system with an inference engine are discussed in Li, D., 1984, A Prolog Database System, Research Studies Press, John Wiley. . .

DETDESC:

DETD(89)
(iii) As the third alternative, we considered an architecture where a multilevel **relational** **database** system was augmented with an inference engine. Such an architecture would be useful as the multilevel **relational** **database** system would ensure the enforcement of a basic mandatory security policy. The inference engine then needs to implement only the. . .

DETDESC:

DETD(92)

Once we had settled on the architecture, the next task was to select a multilevel **relational** **database** system for the implementation. After investigating the various systems that were available, we selected the Secure SQL Server Sybase Inc.. . .

DETDESC:

DETD(107)

This . . . security level from the user. Since we assume that the operating system is secure, we rely on the identification and **authentication** mechanism provided by the operating system. Due to this feature, P1 need not be a trusted process. It operates at. . .

DETDESC:

DETD(279)

An . . . should be handled during query and update processing Stachour, P., and B. Thuraisingham, June 1990, "Design of LDV--a Multilevel Secure **Relational** **Database** Management System," IEE Transactions on Knowledge and Data Engineering, Volume 2, No. 2. However, none of the work reported so. . .

US PAT NO: 5,261,102 [IMAGE AVAILABLE] L8: 4 of 5
US-CL-CURRENT: **395/186**; 340/825.31; 364/246.6, 246.8, 282.1, 282.2, 283.4, DIG.1; 380/25

SUMMARY:

BSUM(20)

An "rdb" is an acronym for "**relational** **database**".

SUMMARY:

BSUM(40)

The . . . directly in some other way. For example, rather than displaying the access privileges, these privileges may be used as an **authentication** mechanism, giving the user direct access to the objects he or she specifies. Alternatively, the information can be used for. . .

DETDESC:

DETD(6)

Specifically, the Database Manager is a database management system (hardware and software) that supports a **relational** **database** model in which all data is viewed as a collection of tables. The Database Manager provides a relational command processor. . . and export of data from and to another computer system; and a system for backup and restoration of an individual **relational** **database** table, and for maintenance.

DETDESC:

DETD(26)

In . . . the name is followed by a blank. The default value is "*". The term "rdb" in the table stands for "**relational** **database**".

US PAT NO: 5,113,499 [IMAGE AVAILABLE] L8: 5 of 5
US-CL-CURRENT: 340/825.34; 364/222.2, 222.3, 222.81, 222.82, 231, 237.2, 237.3, 239.9, 240, 240.8, 240.9, 242.94, 242.96, 259, 259.2, 260.4, 260.81, 262, 262.1, 270.5, 282.1, 283.4, 284, 284.1, 284.3, 284.4, 286.4, 286.5, DIG.1; 370/420; 379/95; **395/726**

SUMMARY:

BSUM(16)

U.S. . . . a PIN, are encrypted using a session key which itself is decrypted using a master key, and then a message **authentication** code is computed using the same session key for other data elements of the message. An acquirer station with which. . .

SUMMARY:

BSUM(18)

U.S. Pat. No. 4,349,695 to Morgan describes an **authentication** system in which the receiver interrogates the transmitter in code. Multiple back and forth transmissions are required to authenticate the. . .

DETDESC:

DETD(4)

To . . . as 7. As will be described in detail presently, TAMS 8 includes an administrative host (AH) together with a master **relational** **database** pertaining to network customers, including user IDs, passwords, and other relevant information, and a validation host (VH) for running software. . .

DETDESC:

DETD(5)

By . . . procedure by which the information is reviewed and a determination is made, based in part on data stored in the **relational** **database**, whether the user will be allowed to access the addressed host or other destination sought to be accessed in the. . .

DETDESC:

DETD(6)

If . . . essence, informs the switch 7 that this user is valid and the requested connection is to be made. The TAMS **relational** **database** correlates all authorized users, their attributes, passwords, and so forth, to addresses to which they are permitted access, among other. . .

CLAIMS:

CLMS(4)

4. . . .
requests for access received thereby,
administrative host computer means coupled to the validation host computer means for monitoring the respective requests, and
relational **database** means associated with said validation host computer means and said administrative host computer means for storing information regarding authorized users,. . .

CLAIMS:

CLMS(7)

7. . . .
terminals and host computers on demand by authorized users,
installing in association with said network an access management host computer and **relational** **database** designating authorized users and their attributes and destination addresses to which the various users are authorized access based on said. . . and issuing instructions respecting establishment of connections and disconnections to the respective switch means based on information contained in said **relational** **database**, and
providing a data link between said access management host computer and each of said switch means for communication of access. . .
=